UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/711,783 | 11/13/2000 | Hugo Fruchauf | 48922.20001.00 | 7175 |

25224 7590 04/21/2006

MORRISON & FOERSTER, LLP
555 WEST FIFTH STREET
SUITE 3500
LOS ANGELES, CA 90013-1024

| EXAMINER | |
|---|---|
| DADA, BEEMNET W | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

DATE MAILED: 04/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/711,783 | FRUEHAUF ET AL. | |
| | Examiner | Art Unit | |
| | Beemnet W. Dada | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *31 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-5,8-11,13-18,24,38-40,47 and 61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-5 and 8-11* is/are allowed.

6)☒ Claim(s) *16-18,24,38-40,47 and 61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/21/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. This office action is in reply to an amendment filed on January 31, 2006. Claims 16, 17, 38, 39 and 61 have been amended and claims 6-7, 12-15, 19-23, 25-37, 41-46 and 48-60 have been cancelled. Claims 1-5, 8-11, 13-18, 24, 38-40, 47 and 61 are pending.

### *Claim Rejections - 35 USC § 102*

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 16-18, 24, 38-40 and 47 are rejected under 35 U.S.C. 102(e) as being anticipated by Kuroda et al US Patent 6,915,434 B1 (hereinafter Kuroda).

4. As per claims 16 and 38, Kuroda teaches a method of cryptographic communication comprising the steps of:

storing in a memory a unique seed (i.e., for example an ID of a data storage apparatus) and a common seed (i.e., for example group ID) [column 9, lines 43-59 and column 10, lines 7-17];

generating a unique cryptographic key using the unique seed [column 9, lines 43-59];

generating a common cryptographic key using the common key [column 10, lines 7-17];

receiving a signal, detecting whether the signal is a unicast signal or a multicast signal, selecting the unique cryptographic key if the signal received is detected to be a unicast signal [column 6, lines 9-24], selecting the common cryptographic key if the signal received is detected

to be a multicast signal [column 6, lines 9-44], and applying the selected cryptographic key to the received signal [column 6,lines 19-56].

5. As per claims 18, 24, 40 and 47, Kuroda further teaches the step of determining whether a signal is encrypted and further comprising transmitting a user address or user identification [column 6, lines 26-35 and lines 45-55].

6. Claim 61 is rejected under 35 U.S.C. 102(e) as being as being anticipated by Wright et al. US Patent 6,084,969 (hereinafter Wright)

7. As per claim 61, Wright teaches a method of cryptographic communication using a system having a plurality of user communication interfaces and a master station, comprising the steps of:

receiving an encrypted signal from one of the user communication interfaces, said encrypted signal addressed to be received by another one of the user communication interfaces, and said encrypted signal being encrypted using a cryptographic key generated by a string generator of said on user communication interface as a function of the unique seed value of said one user communication interface [column 11, lines 30-57];

determining the identification of said one user communication interface sending the encrypted signal [column 12, lines 1-13];

retrieving, from the memory of the master station, the unique seed value corresponding to the identified one user communication interface [column 12, lines 1-13];

generating a cryptographic key using the unique seed value retrieved that corresponds to the identified one user communication interface, decrypting said encrypted signal using said generated key [column 12, lines 1-14];

determining the identification of the other user communication interface, retrieving, from the memory of the master station, the unique seed value corresponding to the other user communication interface, generating a key using the retrieved unique seed value corresponding to the other user communication interface [column 12, lines 27-47];

re-encrypting the decrypted signal using the cryptographic key generated using the retrieved unique seed value corresponding to the other user communication interface, and transmitting the re-encrypted signal to the other communication interface [column 12, lines 43-59].

### *Claim Rejections - 35 USC § 103*

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 17 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kuroda US Patent 6,915,434 B1 in view of Jones US Patent 5,412,730.

10. As per claims 17 and 39, Kuroda teaches the method as applied to claims 16 and 38 above. Kuroda is silent on pseudo-random string generator. However, the use of pseudo-random string generator is old and well known in the art. For example, Jones teaches a cryptographic system including key generation method using pseudo-random string generator

[see figure 1]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Jones within the system of Kuroda in order to generate keys and randomly alter the generated keys.

### *Allowable Subject Matter*

11. Claims 1-5 and 8-11 are allowed.

### *Response to Arguments*

12. Applicant's arguments filed January 31, 2006 have been fully considered but they are not persuasive. Applicant argued that Kuroda does not teach a cryptographic communication method in which received signal is detected to be a particular type of signal such as unicast signal or a multicast signal. Applicant further argued that Kuroda fails to teach selecting different types of cryptographic keys dependent on whether the received signal is detected to be a unicast signal or multicast signal. Examiner disagrees.

13. Examiner would point out that Kuroda teaches a method of cryptographic communication including generating a unique cryptographic key using the unique seed [column 9, lines 43-59], generating a common cryptographic key using the common key [column 10, lines 7-17], receiving a signal, detecting whether the signal is a unicast signal or a multicast signal, selecting the unique cryptographic key if the signal received is detected to be a unicast signal [column 6, lines 9-24], selecting the common cryptographic key if the signal received is detected to be a multicast signal [column 6, lines 9-44], and applying the selected cryptographic key to the received signal [column 6,lines 19-56].

14. With respect to claim 61, applicant argued that Wright does not contain any disclosure of generating, in situ, the cryptographic keys at both the sender and the receiver end of a transmission. Examiner disagrees.

15. Examiner would point out that Wright teaches receiving an encrypted signal from one of the user communication interfaces, said encrypted signal addressed to be received by another one of the user communication interfaces, and said encrypted signal being encrypted using a cryptographic key generated by a string generator of said on user communication interface as a function of the unique seed value of said one user communication interface [column 11, lines 30-57], retrieving, from the memory of the master station, the unique seed value corresponding to the identified one user communication interface [column 12, lines 1-13], generating a cryptographic key using the unique seed value retrieved that corresponds to the identified one user communication interface, decrypting said encrypted signal using said generated key [column 12, lines 1-14]. Examiner asserts that the prior art on record teaches the claim limitations and therefore the rejection is respectfully maintained.

## *Conclusion*

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

April 14, 2006

HOSUK SONG
PRIMARY EXAMINER